

Contents

Preface	<i>page</i> ix
Abbreviations and Standard Notation	xi
Authors	xv
Part 1. Protocols	
Chapter I. Elliptic Curve Based Protocols	
<i>N.P. Smart</i>	3
I.1. Introduction	3
I.2. ECDSA	4
I.3. ECDH/ECMQV	8
I.4. ECIES	12
I.5. Other Considerations	18
Chapter II. On the Provable Security of ECDSA	
<i>D. Brown</i>	21
II.1. Introduction	21
II.2. Definitions and Conditions	23
II.3. Provable Security Results	32
II.4. Proof Sketches	33
II.5. Further Discussion	36
Chapter III. Proofs of Security for ECIES	
<i>A.W. Dent</i>	41
III.1. Definitions and Preliminaries	42
III.2. Security Proofs for ECIES	50
III.3. Other Attacks Against ECIES	58
III.4. ECIES-KEM	61

Part 2. Implementation Techniques**Chapter IV. Side-Channel Analysis***E. Oswald*

IV.1. Cryptographic Hardware	69
IV.2. Active Attacks	70
IV.3. Passive Attacks	71
IV.4. Simple SCA Attacks on Point Multiplications	72
IV.5. Differential SCA Attacks on Point Multiplications	77
	84

Chapter V. Defences Against Side-Channel Analysis*M. Joye*

V.1. Introduction	87
V.2. Indistinguishable Point Addition Formulae	87
V.3. Regular Point Multiplication Algorithms	88
V.4. Base-Point Randomization Techniques	93
V.5. Multiplier Randomization Techniques	97
V.6. Preventing Side-Channel Analysis	98
	100

Part 3. Mathematical Foundations**Chapter VI. Advances in Point Counting***F. Vercauteren*

VI.1. p -adic Fields and Extensions	103
VI.2. Satoh's Algorithm	104
VI.3. Arithmetic Geometric Mean	105
VI.4. Generalized Newton Iteration	115
VI.5. Norm Computation	121
VI.6. Concluding Remarks	128
	132

Chapter VII. Hyperelliptic Curves and the HCDLP*P. Gaudry*

VII.1. Generalities on Hyperelliptic Curves	133
VII.2. Algorithms for Computing the Group Law	133
VII.3. Classical Algorithms for HCDLP	136
VII.4. Smooth Divisors	140
VII.5. Index-Calculus Algorithm for Hyperelliptic Curves	142
VII.6. Complexity Analysis	144
VII.7. Practical Considerations	146
	149

Chapter VIII. Weil Descent Attacks*F. Hess*

VIII.1. Introduction – the Weil Descent Methodology	151
VIII.2. The GHS Attack	151
VIII.3. Extending the GHS Attack Using Isogenies	153
	166

VIII.4. Summary of Practical Implications	173
---	-----

VIII.5. Further Topics	175
------------------------	-----

Part 4. Pairing Based Techniques**Chapter IX. Pairings***S. Galbraith*

IX.1. Bilinear Pairings	183
IX.2. Divisors and Weil Reciprocity	183
IX.3. Definition of the Tate Pairing	184
IX.4. Properties of the Tate Pairing	185
IX.5. The Tate Pairing over Finite Fields	187
IX.6. The Weil Pairing	189
IX.7. Non-degeneracy, Self-pairings and Distortion Maps	191
IX.8. Computing the Tate Pairing Using Miller's Algorithm	192
IX.9. The MOV/Frey–Rück Attack on the ECDLP	196
IX.10. Supersingular Elliptic Curves	197
IX.11. Applications and Computational Problems from Pairings	198
IX.12. Parameter Sizes and Implementation Considerations	201
IX.13. Suitable Supersingular Elliptic Curves	203
IX.14. Efficient Computation of the Tate Pairing	204
IX.15. Using Ordinary Curves	205
Appendix: Proof of Weil Reciprocity	208
	212

Chapter X. Cryptography from Pairings*K.G. Paterson*

X.1. Introduction	215
X.2. Key Distribution Schemes	215
X.3. Identity-Based Encryption	218
X.4. Signature Schemes	221
X.5. Hierarchical Identity-Based Cryptography and Related Topics	228
X.6. More Key Agreement Protocols	235
X.7. Applications and Infrastructures	240
X.8. Concluding Remarks	242
	250

Bibliography

Summary of Major LNCS Proceedings	253
	271

Author Index**Subject Index**

273

277